



realtimepublishers.com[™]

The Definitive Guide[™] To

Exchange 2000 Design
and Deployment

ælitTMa

SOFTWARE

Evan Morris

Chapter 4: Exchange 2000 Migration in a Multi-Forest Environment	90
Migration.....	90
Directory Services and the GAL.....	91
Authentication Between Domains and Forests.....	92
AD Inter-Forest Trust	94
Installing Exchange 2000.....	96
E2KDSInteg.....	98
Assessing Migration Products.....	98
LDAP-Based Tools.....	99
The ADC.....	100
Exchange 5.5 Container Topologies.....	101
The ADMT.....	103
ADClean	104
Moving Mailboxes.....	106
Microsoft Exchange Migration Wizard	107
Mailbox Migration Tips.....	110
Single Instance Storage.....	111
Validation Procedures.....	111
Public Folders	112
Client Desktops and Outlook Profiles.....	112
Other Migration Considerations	113
Summary	113

Copyright Statement

© 2002 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

Chapter 4: Exchange 2000 Migration in a Multi-Forest Environment

In the previous chapter, we examined the Exchange 2000 upgrade and migration strategies, then spelled out the exact procedures for an in-place upgrade. We also defined the risks involved with this method and why you might want to perform a migration instead.

In this chapter, we will look at migration in great detail—covering the tools and methods of the migration process. The goal of migration is to migrate either a single Exchange 5.5 organization or multiple Exchange 5.5 organizations to either a single AD forest or multiple AD forests. This migration strategy provides you with an opportunity to design a new Exchange topology. In addition, this design can be maintained for a long-term period with the intent of splitting off the organization at a later date.

Migration

The following list highlights the key concepts that we will cover for a migration:

- Directory services and the GAL
- Authentication between domains and forests
- Installing Exchange 2000
- Migration tools
- Moving mailboxes
- Public folders
- Client desktops and Outlook profiles
- Additional migration considerations

The migration process consists of migrating user accounts to AD, synchronizing the Exchange 5.5 directory (mailbox properties), installing Exchange 2000 and establishing coexistence, then moving the mailbox and account information to Exchange 2000 and AD. Fortunately, the steps are somewhat flexible—although this list is the suggested order. The main thing to keep in mind is that the infrastructure needs to be in place for directory synchronization and authentication so that users are not left stranded when they are moved to the new system.

Starting with Exchange 2000 Service Pack 1 (SP1), the Microsoft Exchange Migration Wizard can move mailboxes from one Exchange Server 5.5 organization to a separate Exchange 2000 organization. The Exchange 5.5 server can even be located in the same forest as the target Exchange 2000 organization, but only if the Exchange 2000 organization is not joined to the source Exchange 5.5 organization and has a different organization name.

Although this chapter deals with the Microsoft-available tools, you have the option to select a robust, third-party tool. I will discuss the advantages of third-party tools later in this chapter.

When run in inter-organization mode, the ADC creates contacts in AD with email addresses for the Exchange 5.5 organization. This functionality lets Exchange 2000 and AD users send email during the migration process. The ADMT migrates account permissions (the NT SID on printers, file shares, and mailboxes) and creates new user accounts. However, the ADMT does not match the new accounts with the existing contacts created by the ADC, so we must use the Active Directory Account Cleanup Wizard. ADClean merges the user accounts (from the ADMT) with the contacts (from the ADC), creating mail-enabled user accounts. Next, the Exchange Migration Wizard (from the most recent Exchange 2000 service pack) changes the user accounts to mailbox-enabled users, creates the Exchange 2000 mailboxes, then migrates the Exchange 5.5 data to the new mailboxes.

Directory Services and the GAL

The first step in the inter-organization migration process consists of migrating user accounts to AD, so we will obviously need AD in place. (I discussed AD essentials in the previous chapters.) A solid directory is the foundation for a successful migration project, so give as much focus as possible to this area.

Before proceeding with the migration, ensure that the target domain in AD has been converted to native mode. Remember that this process is irreversible, so you will no longer be able to join NT 4.0 domain controllers to this domain. The native-mode domain is required for creation of Universal Security Groups (USGs) and will be used by both the ADMT and the ADC. Figure 4.1 shows the dialog boxes you will go through during the process of changing to native mode. Is native mode an absolute requirement? No, but unless you can guarantee that no Public Folder permissions are set via distribution lists (DLs), then a native-mode domain is very strongly suggested.

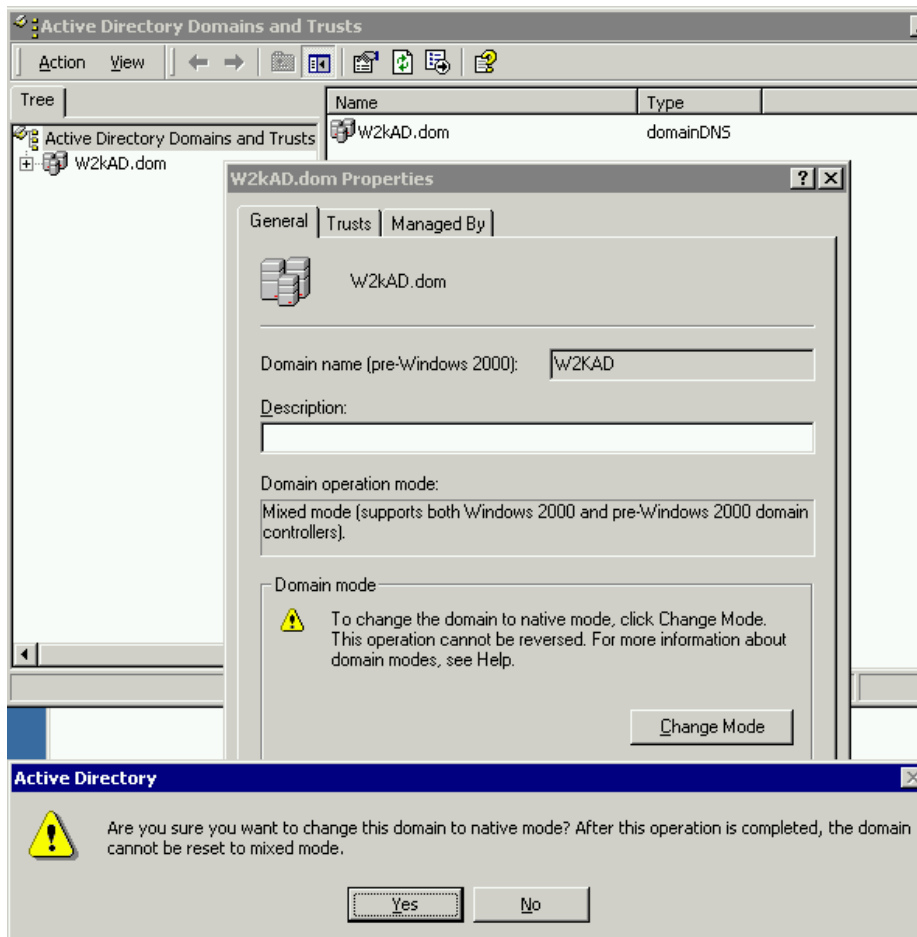


Figure 4.1: Changing to native-mode to support USGs.

Authentication Between Domains and Forests

Because the NT domain(s) and the AD forest(s) are separate authentication authorities, we will need to establish trust between them. One of the primary migration tools, the Exchange Migration Wizard, requires a working trust relationship between the source and target domains (and so does the ADMT). In AD, the trust is created using the AD Domains and Trusts Microsoft Management Console (MMC) snap-in. In NT 4.0, the trust is created using User Manager for Domains by selecting Policies, Trusts. Figure 4.2 shows the first step of adding the NT domain as a trusting domain to the AD domain.

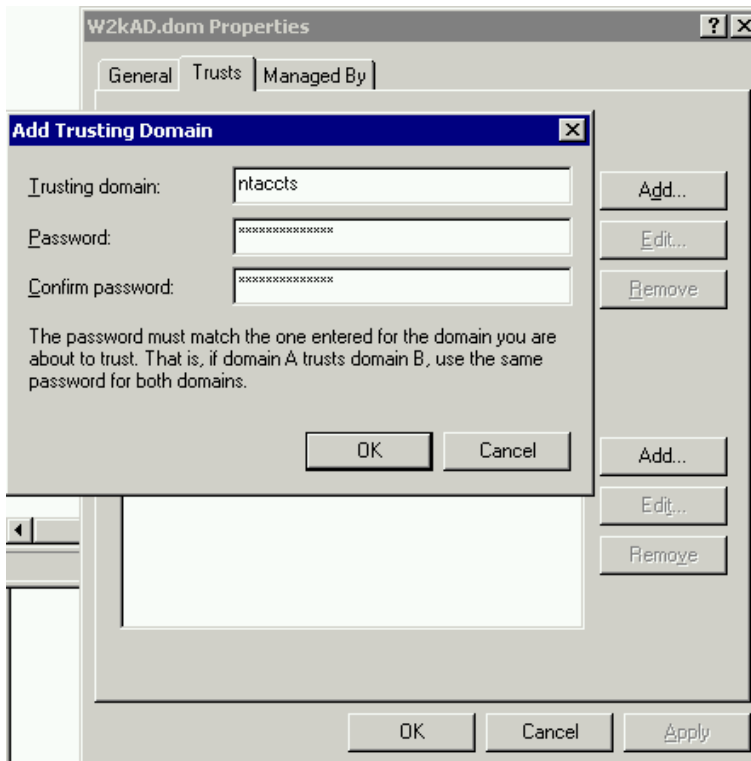


Figure 4.2: Adding an NT domain as a trusting domain.

When you add an NT domain as a trusting domain, you will be presented with the pop-up message that Figure 4.3 shows to verify the new trust.

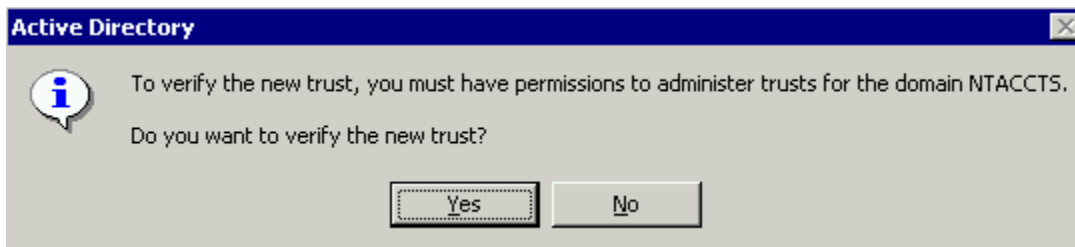


Figure 4.3: Trust verification message.

When the trust has been verified, you will receive the following message (see Figure 4.4) that lets you know that the trust creation was successful.

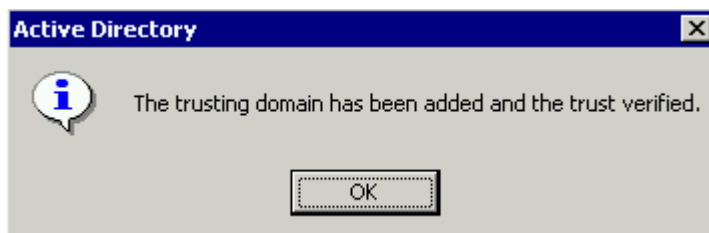


Figure 4.4: Successful completion of trust creation.

AD Inter-Forest Trust


What about the scenario in which Exchange 2000 exists in a different forest than the AD accounts? In this scenario, often referred to as deploying Exchange 2000 in a *resource forest*, our AD topology is similar to the common deployment scenario for NT domains using a master account domain and an Exchange resource domain. The big difference is that Exchange 2000 expects the mailbox to be associated with an account in the same forest (again, another subtle but significant difference is that in Exchange 5.5, it was the account that was associated with the mailbox).

For the inter-forest deployment to work, we must create an explicit trust relationship between the AD domain containing the accounts and the AD domain containing the Exchange servers (in the other forest) much like we did with NT domains. In addition, the administrator creating the accounts and mailboxes in the account forest will need to have administrative access to the Exchange resource forest. Remember from previous chapters the idea of adding the Everyone group to the *Pre-Windows 2000 Compatible Access* security group? This setting is an important security configuration for allowing inter-forest read access to the directory.

Usually Exchange 2000 mailboxes are associated with AD user accounts in the same forest. However, it is possible to configure Exchange 2000 mailboxes to be associated with NT 4.0 domain accounts. When you run the ADC, then move a mailbox to Exchange 2000, the account may still be an NT 4.0 domain account. There will normally be a disabled AD account for the user with the `msExchMasterAccountSID` attribute set to the SID of the NT 4.0 account.

The process for linking an account domain to Exchange in another forest involves creating a placeholder account and setting the special Associated external account permission. Figure 4.5 shows the Associated external account permission set on the placeholder account.


First, you should create or already have the user account in the trusted AD forest. Next, create the mailbox-enabled account in the Exchange forest (technically, the account exists in a domain in that forest). Right-click the newly created account, and select *Disable Account*. Get the `msExchMasterAccountSID` attribute from the first AD account, and set it on the mailbox-enabled user account. Doing so can best be accomplished programmatically or with an account cloning tool (for example, `ClonePrincipal` or `ADMT`). In fact, if a mailbox-enabled disabled account does not have the `msExchMasterAccountSID` attribute, then mail will not be delivered to it, and instead will be returned with a non-delivery receipt (NDR).

 For a code sample to set the `msExchMasterAccountSID` attribute on the mailbox-enabled user account, see the Microsoft article "HOW TO: Associate an External Account with an Existing Exchange 2000 Mailbox" (Q322890). You must register the `ADsSecurity.dll` file on the system on which you will run the script by entering

```
C:\winnt\system32\regsvr32 ADsSecurity.dll
```

Also, the code must be run on an Exchange 2000 Server with SP2 or later or SP1 with the hotfix referenced in the Microsoft article "XADM: You Cannot Programmatically Change Mailbox Rights" (Q302926).

Next, modify the ACL of this account to add the external AD account by doing the following: Open the account properties, select the Security tab, and click Add. Select the account from the other forest (you must have the trust set up properly for this to work), and select the Allow check box next to Send As permissions, then click OK. Next, select the Exchange Advanced tab, then click Mailbox Rights. (If you do not see the Exchange Advanced tab, then close the account, select View, then click Advanced Features in the Active Directory Users and Computers MMC snap-in). Click Add, select the external account, then click OK. Select the Allow permissions for Read Permissions, Full Mailbox Access, and Associated external account.

 In spite of all my previous praise of Exchange 2000 SP3, I must add this note: In a multiple forest topology, SP3 causes a problem for OWA users. If your OWA users begin receiving the `Http://1.1 401 Unauthorized` error message, you need to check for the SELF account and remove it from their account permissions.

The SELF account exists in all Win2K domains and uses well-known SIDs that can be set on generic accounts. To check for the SELF account, open the account property for the disabled account, and select the Exchange Advanced tab. (Again, you must have enabled View, Advanced Features in the Active Directory Users and Computers MMC snap-in). Click Mailbox Rights, and scroll through the list of account names to make sure that the only account with the Associated external account permission selected is the user's matching the account in the other forest.

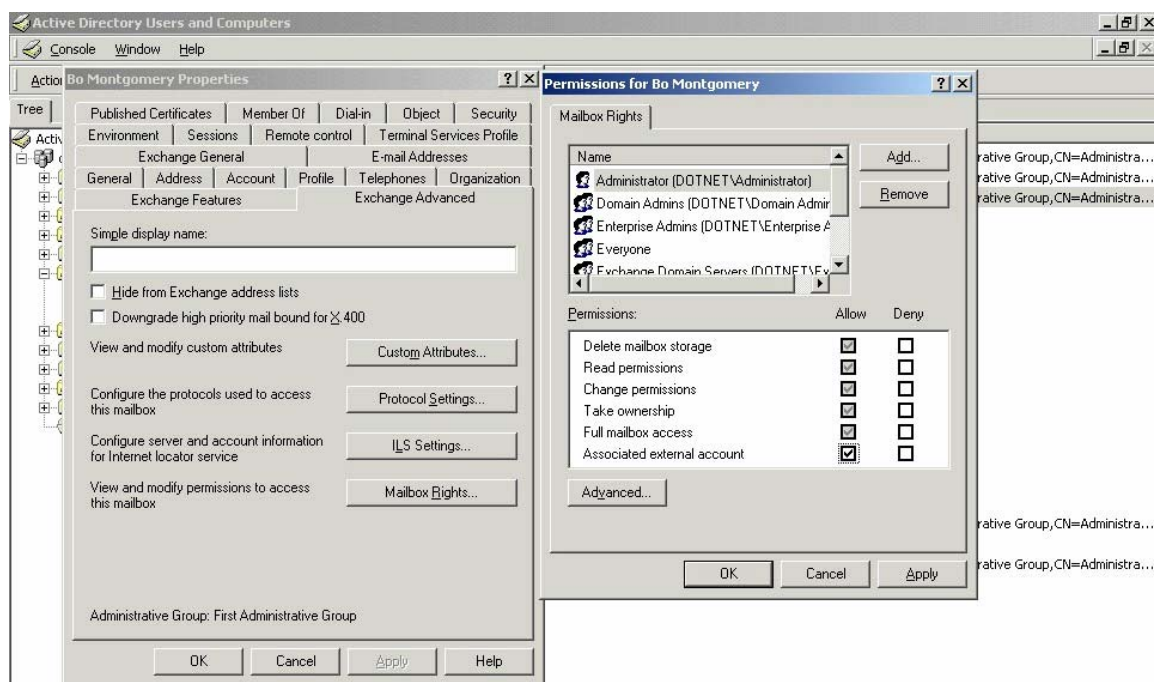


Figure 4.5: Placeholder account and associated external account permission.

You must also consider a few other implications of the multi-forest design that will impact your support procedures, such as the effect on searching for objects across multiple forests. By default, GC servers build a subset of information for all domains in the forest; however, your new enterprise directory will consist of domains that the GC does not replicate information with. For users to search across all forests, they must explicitly state the domain names, so they must be educated on how and when to do so. The alternative is to implement a meta-directory or directory synchronization solution, but you will have to weigh the added complexity of such a solution against the benefit to end users.

Installing Exchange 2000

In the previous chapters, we have covered many things that you should know before installing Exchange 2000 (such as running NLTest and DCdiag). The crucial difference between an intra-organization and inter-organization migration is the step in the Exchange 2000 installation wizard that Figure 4.6 shows. In the case of an inter-organization migration, you will create a new organization instead of joining Exchange 2000 to the existing Exchange 5.5 organization.

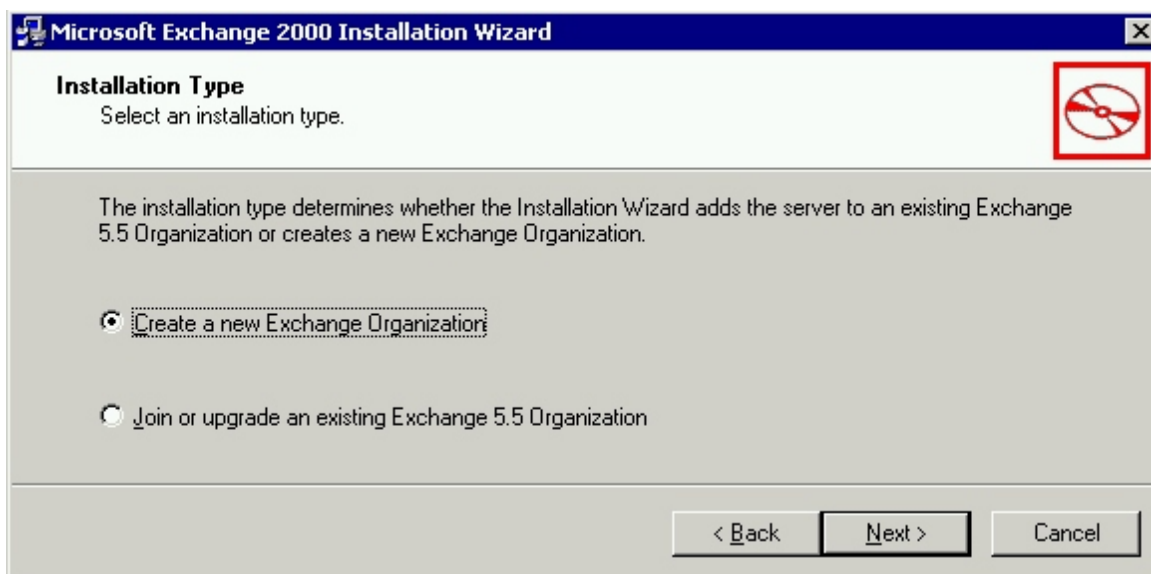


Figure 4.6: Choice when installing the first Exchange 2000 server.

Depending on the choices that you made when you installed AD, you might next see the pop-up message that Figure 4.7 shows. What does this message mean? Your domain might be identified as an *insecure domain for mail-enabled groups with hidden membership*, meaning that distribution group membership (the Exchange 2000 equivalent of DLs in Exchange 5.5) will be readable even if you have attempted to hide the membership. The reason, in a nutshell, is that the Everyone group is added to the *Pre-Windows 2000 Compatible Access* security group. This group is used by the Internet Authentication Service (IAS) and is necessary whenever there is a mix of NT 4.0 domains and remote access. There is a specific circumstance when a remote user connecting via any RRAS method such as dial-up or virtual private network (VPN),

connects to an NT 4.0 server that must then authenticate the user against AD. The computer uses its own account to impersonate the user and attempt authentication, which fails unless the Everyone group has access to read AD contents. The result is that if Everyone has access to read AD content, even your hidden membership is readable. If this issue is a concern, you must decide whether you need to provide RRAS authentication in a mixed NT 4.0 and Win2K environment.

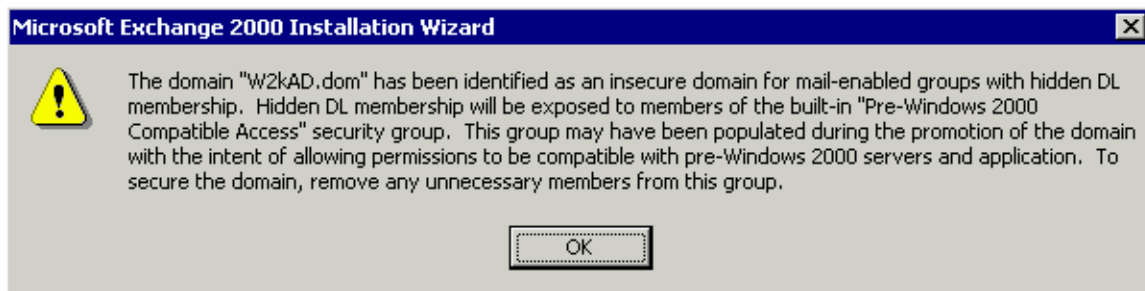


Figure 4.7: Insecure domain for hidden mail-enabled groups.

As part of the Exchange 2000 installation, a program group will be created with the following essential tools (see Figure 4.8):

- Active Directory Cleanup Wizard—We will use this tool as part of our inter-organization migration process.
- Active Directory Users and Computers MMC snap-in—This tool replaces the functionality of NT 4.0 domains (User Manger for Domains and Exchange 5.5 Administrator console) for creating users accounts and mailboxes in AD.
- Migration Wizard—We will use the Microsoft Exchange Migration Wizard that is updated by the latest Exchange service pack for inter-organization mailbox moves.
- System Manager—Also referred to as the Exchange System Manager (ESM), this tool is the replacement for the Exchange 5.5 Administrator console. You can use the ESM to define Exchange 2000 Admin Groups ahead of time for your entire organization so that servers can be directly installed into the correct Admin Group (although you must select the correct Admin Group, the process is not automatic).
- Active Directory Migration Tool—This tool is installed as part of the Win2K resource kit.



Figure 4.8: Essential tools installed in the Microsoft Exchange Start menu.

The following sections explore additional Exchange 2000 migration tools as well as considerations for purchasing third-party tools.

E2KDSInteg

After installing the first Exchange 2000 server as well as at other crucial points in the migration (such as after setting up each of the migration tools we will cover in this chapter), I recommend running the E2KDSInteg utility. This tool checks the health of AD, accounts, and mailboxes after Exchange 2000 or the ADC has been installed. It generates or appends to a text report (e2kdsinteg.log) that you can check for errors. E2KDSInteg can uncover some odd errors and problems; for example, missing account properties such as having no home MDB (database) set for a mailbox. If you find errors like this, check the event logs for more detail—there are many errors listed with the documentation for E2KDSInteg that point to issues with the Recipient Update Service (RUS) not properly stamping ADC replicated objects.

To run E2KDSInteg, log on as a domain administrator, run the setup.exe to install E2KDSInteg, then type the following at a command prompt:

```
c:\Program Files\Exchange 2000 DS Integrity Checker>
e2kdsinteg <GC server>
```

where <GC server> is the name of a GC server that you have read access to.

Assessing Migration Products

Rather than do a comparison of third-party migration products—especially because it is a leapfrog game with vendors adding new features with each release—I will provide you with a list of important questions to consider when evaluating migration products:

- What migration scenarios are supported (for example, Exchange 5.5 to Exchange 2000 only)? Does this product support inter-organization migrations?
- What unique features make the product compelling?
- Is it sold as a product or service?

- How does it specifically handle directory, mailbox, and Public Folder migration?
- What additional capabilities does it provide, such as keeping DLs synchronized between organizations?
- How does it handle the ADC—Is the ADC required or optional? Can it co-exist?
- What if I have other tools for LDAP directory synchronization—how does it interoperate?
- What type of reporting status emails and notifications can the administrator receive?
- Does it provide any additional administrative flexibility (such as a single console for managing both systems and the entire operation)?
- What does it take to extend the product for specific needs within my organization?

Although the procedures in this chapter focus on the Microsoft-provided tools, I will point out where they are lacking and third-party migration products excel, leaving you open to select the vendor that meets your needs.

LDAP-Based Tools

I will lump together LDAP-based directory synchronization tools, as they have many similarities, most notably being quite effective and efficient once properly configured. The catch is that proper configuration can require the extensive knowledge of an experienced consultant. For this reason, many of these tools are sold only as part of a consulting package. Such used to be the case for Microsoft Metadirectory Services (MMS) version 2.2, which is now being transitioned to MMS version 3, which will be available as a series of products. One of the benefits of the new version of MMS is an easier to use interface—with a GUI to allow you to select the mapping of attributes between directories. Most directory synchronization tools are script based and you must have the knowledge of what to edit within the scripts. The implementation of directory synchronization tools is most likely not something that you can accomplish in the spare time in your schedule.

SimpleSync from CPS Systems is also becoming a popular tool in the LDAP synchronization tool arena, perhaps because of its ability to synchronize any combination of Exchange 5.5, Exchange 2000, AD, and other systems such as IPlanet, Lotus Domino R5, and Novell NDS. SimpleSync allows for multiple AD forest synchronization and creates mail-enabled disabled user accounts with the SID of the user in the account's forest. This directory synchronization tool can provide two-way synchronization with AD and other sources of information (such as enterprise resource planning—ERP—systems) so that AD can be the central administrative focus.

The ADC

When you define an inter-organization CA (as Figure 4.9 shows), the ADC creates contacts in AD with email addresses for the Exchange 5.5 organization. Doing so lets Exchange 2000 and AD users send email during the migration process.

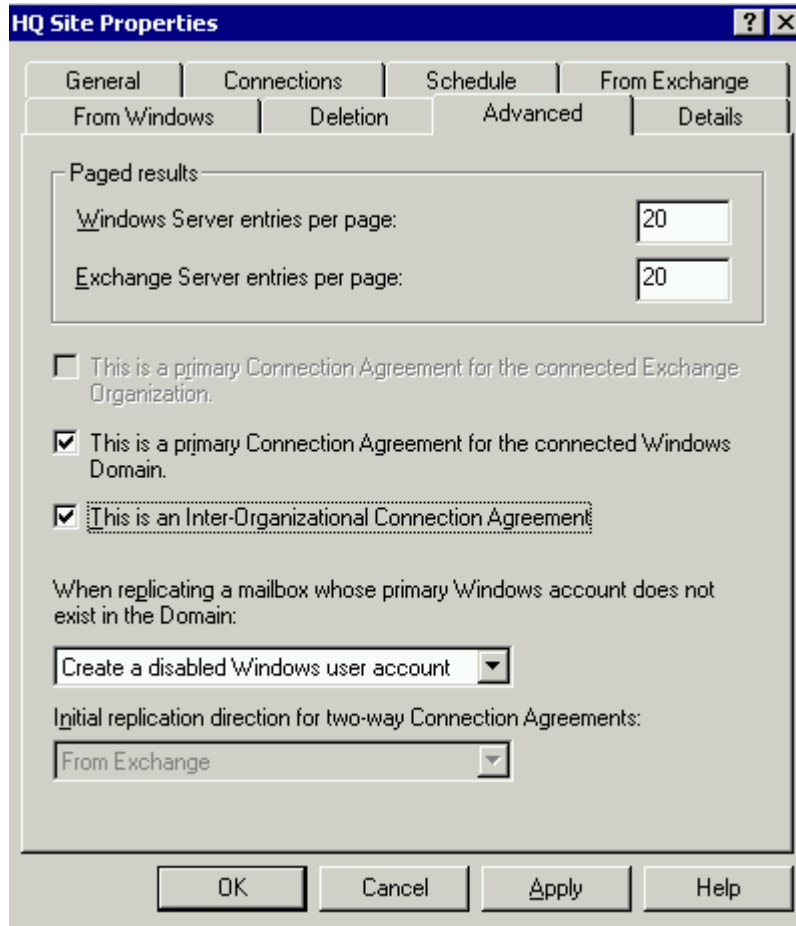



Figure 4.9: Setting up an inter-organizational CA.

To set up an inter-organizational CA, launch the ADC MMC from the Administrative Tools menu. Create a new recipient CA, and give it a descriptive name. On the Advanced tab, select the *This is an Inter-Organizational Connection Agreement* check box.

 If the CA has already been defined, albeit incorrectly, in the details pane, double-click the CA for which you want to choose replication options, and select the *This is an Inter-Organizational Connection Agreement* check box. I have found that you can force replication of Exchange 5.5 mailboxes by updating a single property of each mailbox (which can be done by CSV import, as covered in previous chapters). What you do not want to do is delete the AD replicated objects (see the following caution box).

The inter-organization CA is not available for Public Folder CAs. We will look at inter-organization Public Folder migration in a moment.

🔥 A couple of gotchas to watch out for with the ADC: First, ensure that the ADC connects only to a GC server instead of just an AD domain controller. The GC is critical to ensure uniqueness of a value for the account attribute legacyExchangeDn. Second, make sure that if you create multiple CAs, they do not overlap source or target containers and are marked as a primary CA. If overlap happens, they have the potential to create duplicate objects.

Exchange 5.5 Container Topologies

When configuring a CA in the ADC, the default behavior is that the entire hierarchy of recipient containers will replicate from Exchange 5.5 and be re-created in AD. So you do not need a separate CA for each Exchange 5.5 recipient container; however, there is a situation in which you might want to do so: When you want to reorganize the topology or flatten the recipient containers.

A word of caution about the ADC: One company deploying the ADC did not like the location of replicated objects placed in AD, so they decided to delete them and change the CA. Imagine their shock when they figured out that they had just deleted a large quantity (can you say thousands?) of Exchange 5.5 mailboxes. Needless to say, they had to set up a recovery server and start recovering mailboxes quickly.

Figure 4.10 shows an example of nested recipient containers in Exchange 5.5. (Figure 4.10 also illustrates the Address Book Views, which we will fully cover in the next chapter.)

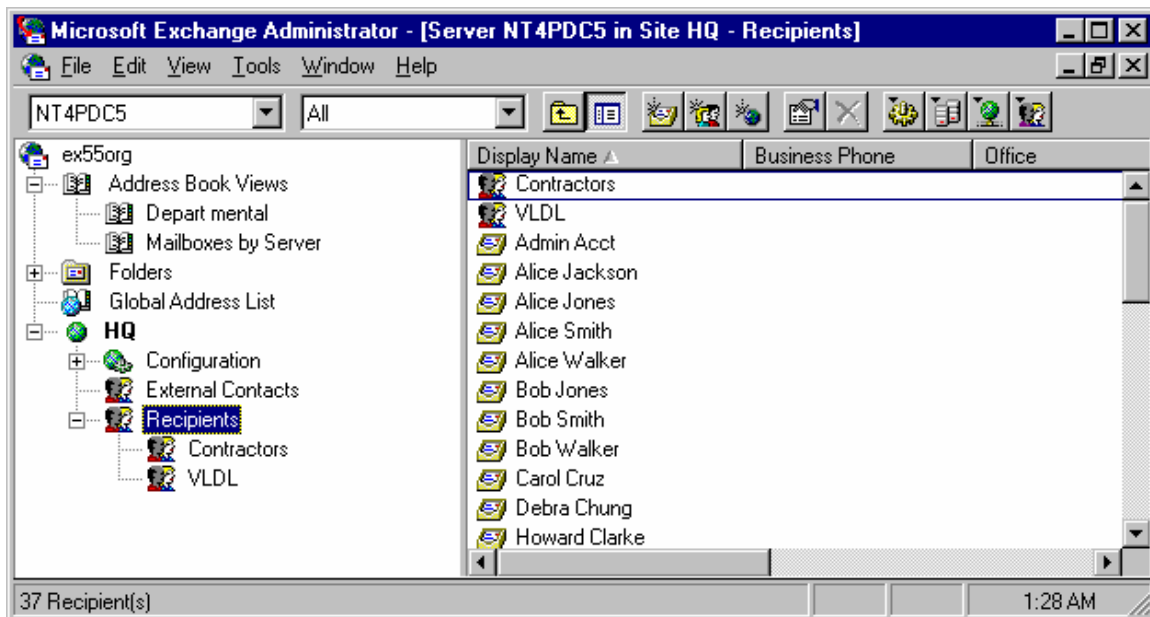


Figure 4.10: Nested recipient containers in Exchange 5.5.

Figure 4.11 shows the result of the nested containers in AD (note that the user objects are disabled accounts instead of just inter-organization contacts).

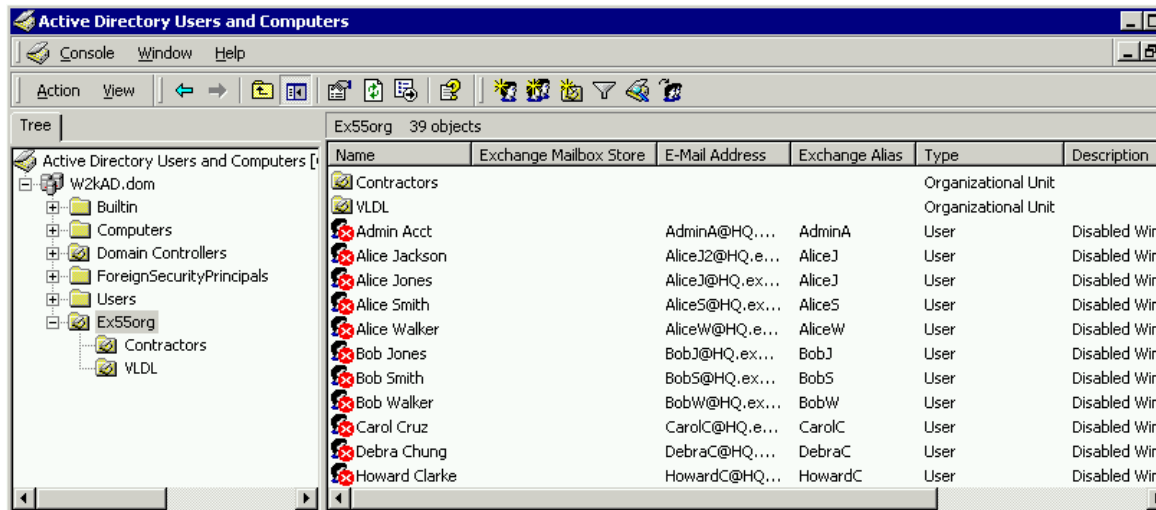


Figure 4.11: Replication of nested recipient containers from Exchange 5.5 to AD via the ADC.

You have control over which attributes will be replicated via the ADC, as Figure 4.12 shows. However, Microsoft advises against using the ADC management interface for creating matching rules. For more information about creating or modifying the ADC matching rules see the Microsoft article “XGEN: How Matching Rules Work in the ADC” (Q269828).

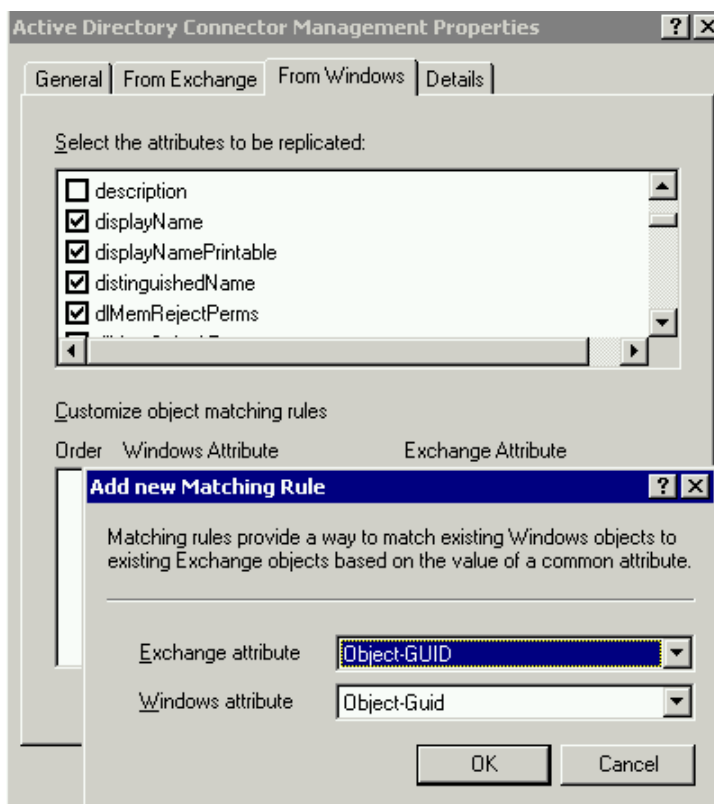


Figure 4.12: ADC attribute selection and matching rules.

The ADMT

Remember that the purpose of the ADMT is to migrate account permissions (the NT SID on printers, file shares, and mailboxes) to new user accounts in AD. Because the ADMT does not match the new accounts with the existing contacts created by the ADC, we must use ADClean if the ADC is run in inter-organization mode. The ADMT will match the account if you use disabled user accounts instead of contacts (as it does in intra-organization mode), but only if the Exchange alias matches the NT account name (which is not always the case). In addition, there are other third-party migration tools that you can use instead of the ADMT.

For the ADMT to migrate account permissions, be sure to select the *Migrate user SIDs to target domain* check box as Figure 4.13 shows. You will also need to ensure that the ADMT wizard is run in the mode to make the actual changes instead of just reporting mode.

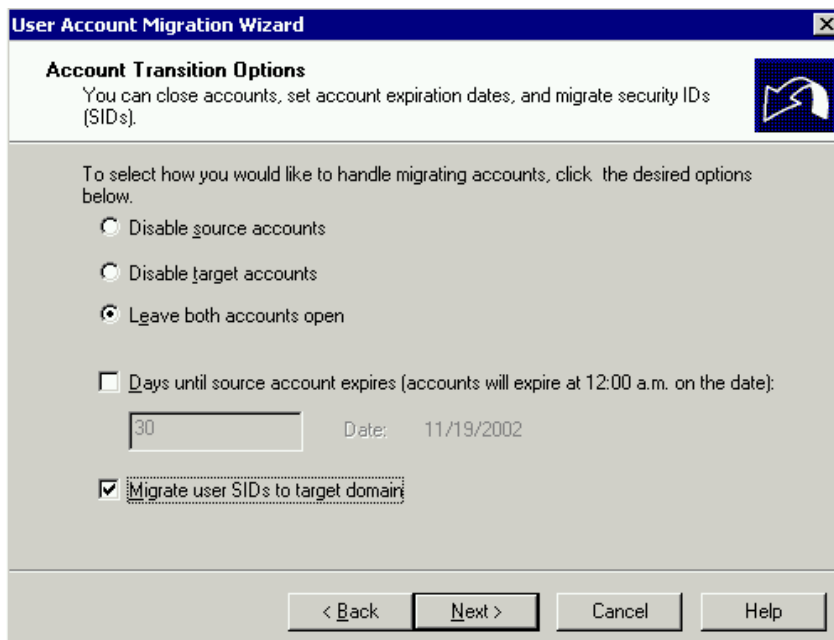


Figure 4.13: Migrating user SIDs with the ADMT.

Until you have configured both domain trusts (as I discussed previously in this chapter), you will be presented with the error message that Figure 4.14 shows.

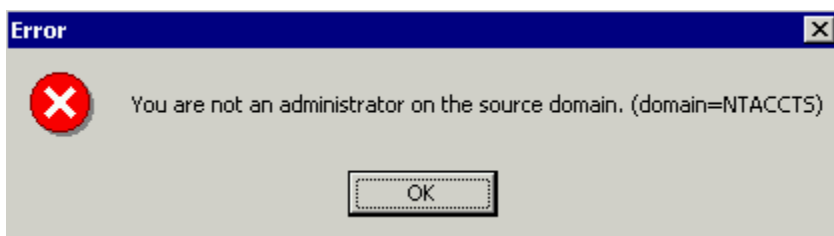


Figure 4.14: Error message you will receive if the trust isn't configured.

The latest version of the ADMT, version 2, has some new features such as the ability to perform inter-forest password migration and INetOrgPerson support. (I'll provide more information about these new features in Chapter 6).

ADClean

ADClean merges the user accounts created by the ADMT with the contacts from the ADC, creating mail-enabled user accounts as a result. This process has the potential to be destructive, so you will see the warning message that Figure 4.15 shows about merging accounts with ADClean.

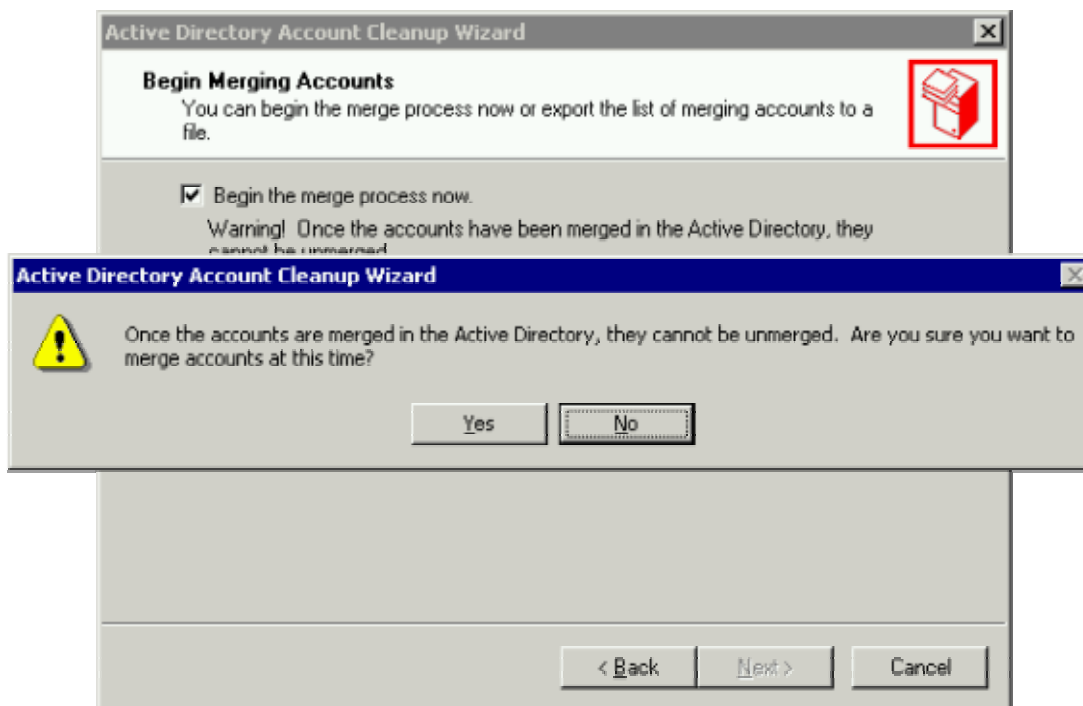


Figure 4.15: Warning about merging accounts with ADClean.

Figure 4.16 shows the view of AD with a duplicate contact and user account before ADClean is run. In this example, I have prepared the user Alice Smith with the ADC, and the ADMT has created an account named ASmith.

Tree		Ex55org 45 objects			
	Name	Type	Description	E-Mail Address	Excha
Active Directory Users and Comp					
W2kAD.dom					
Builtin					
Computers					
Domain Controllers					
Ex55org					
Contractors	Contractors	Organizational ...			
VLDL	VLDL	Organizational ...			
ForeignSecurityPrincipals					
Migrated Users					
Users	Admin Acct	User	Disabled Windows user account	AdminA@ex55o...	Admin
	Alice Jackson	User	Disabled Windows user account	AliceJ2@ex55o...	AliceJ
	Alice Jones	User	Disabled Windows user account	AliceJ@ex55or...	AliceJ
	Alice Smith	Contact		AliceS@ex55or...	Asmith
	Alice Walker	User	Disabled Windows user account	AliceW@ex55or...	AliceW
	ASmith	User			
	Bob Jones	User	Disabled Windows user account	BobJ@ex55org...	BobJ
	Bob Walker	User	Disabled Windows user account	BobW@ex55or...	BobW

Figure 4.16: Duplicate contact and user account before ADClean.

When running ADClean, be sure to clear the *Search based on Exchange mailboxes only* check box (see Figure 4.17) or you will need to manually select the accounts.

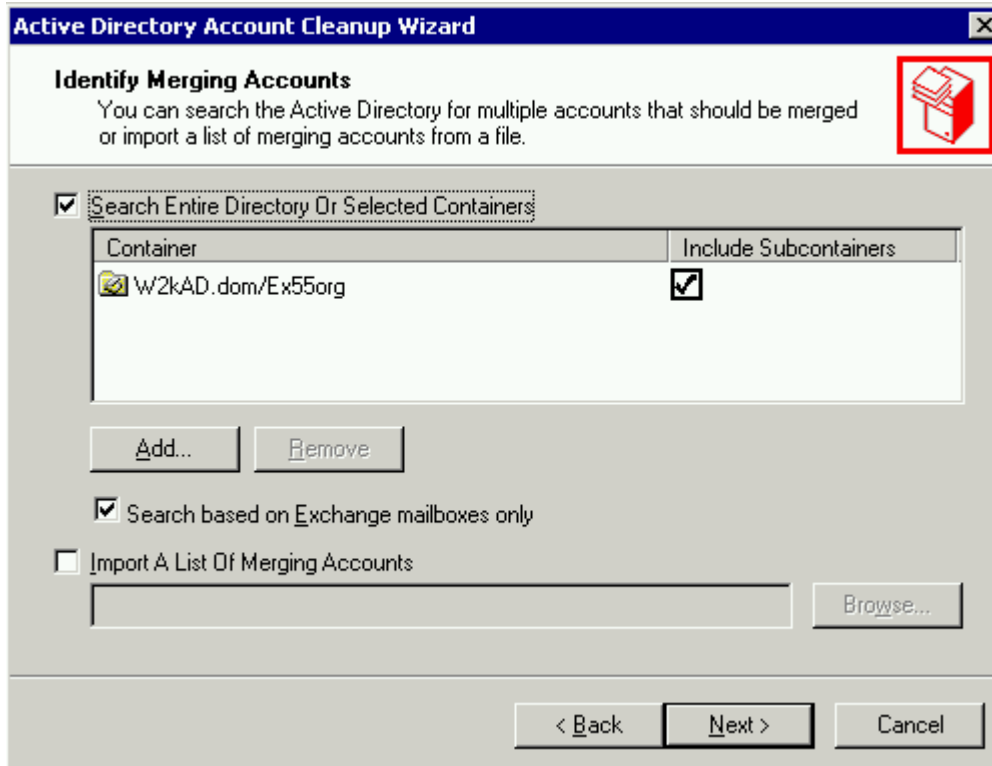


Figure 4.17: Clear the Search based on Exchange mailboxes only check box in ADClean.

If ADClean does not match the contact with the user account, you must manually select each one, as Figure 4.18 shows. When you click Browse, you will be presented with the AD contents to select the user. Select the Name column when browsing for the user, which will sort the contents. Otherwise, when you type in the user name, the contents will not scroll to that user, making it more difficult to find the user.

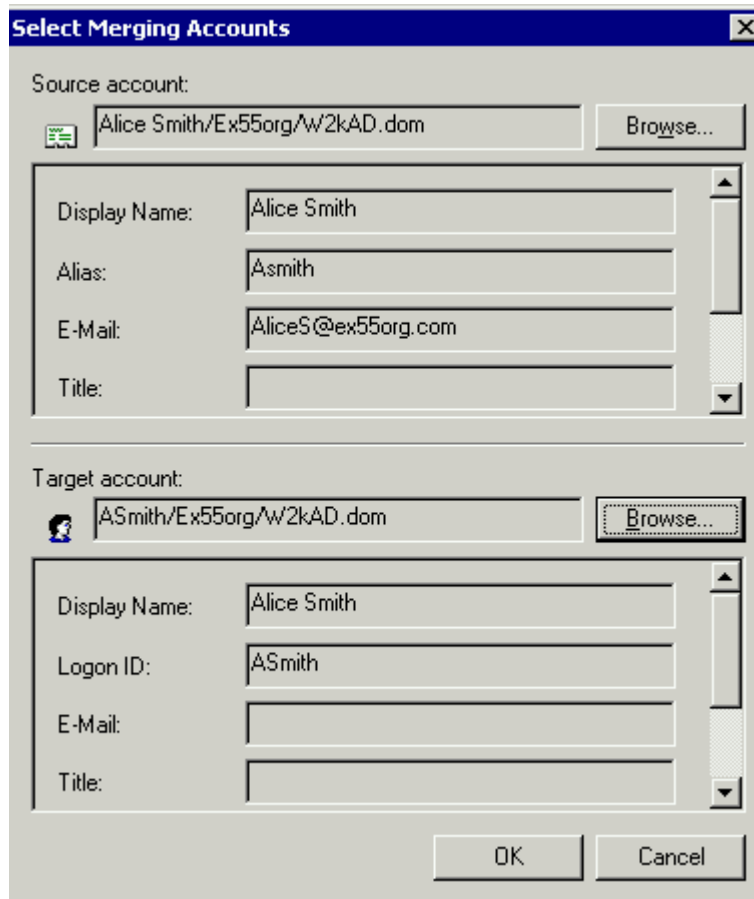


Figure 4.18: Selecting the accounts to be merged by ADClean.

Moving Mailboxes

The main challenges when moving mailboxes are deciding which tools to use, determining how to speed or automate the process, dealing with antivirus scanning, minimizing network impact, and recovering from failed moves. A utility such as the Microsoft Exchange Migration Wizard is essential for migration, as you cannot merely move mailboxes between organizations (using Active Directory Users and Computers). Alternatively, you can use a third-party tool, which gives you quite a few advantages, namely:

- Background migration, including synchronization of the two mailboxes until you're ready to transfer the client from Exchange 5.5 to Exchange 2000.
- Compressed replication of migration traffic.
- Automated update of client (Outlook) profiles.
- *Scheduled* background migration, which lets you sleep or go play outside instead of perfecting your Next, Next, Next mouse-clicking technique under the glow of fluorescent lighting in the wee hours of the morning or over weekends.

In the next section, I'll use the Microsoft Exchange Migration Wizard. However, as you can see from this list, investing in a robust third-party tool offers many advantages.

Microsoft Exchange Migration Wizard

The Microsoft Exchange Migration Wizard can be used to migrate mailboxes from either Exchange 5.5 to Exchange 2000 within an organization or from one Exchange 2000 organization to another Exchange 2000 organization (this feature is available in the SP2 and later versions). The SP2 and later versions also provide the ability to perform two-step migrations with PSTs as the intermediary file, and give you the ability to filter messages during migration based on date, size, and subject line messages.

The Microsoft Exchange Migration Wizard sets the original NT 4.0 source account as the account on the newly migrated Exchange 2000 mailbox. The wizard can create disabled user accounts in the AD target forest that are associated with the source user accounts that connect to the mailboxes. Microsoft does not recommend that you enable these disabled user accounts.


When you run the wizard, select the Exchange Server 5.5 mailboxes that you want to import from the Account Migration page of the wizard. If the mailboxes do not currently exist as users or contacts in AD, the wizard creates new AD users. If an Exchange 5.5 mailbox already exists as a contact (for example, a contact that was created by an inter-organizational CA) in AD, the wizard matches the Exchange 5.5 mailbox with the contact, then converts the contact to a disabled AD user account.

Next, the wizard (from the most recent Exchange 2000 service pack) changes the user accounts to mailbox-enabled users, creates the Exchange 2000 mailboxes, then migrates the Exchange 5.5 data to the new mailboxes. The wizard searches AD for user objects with SIDs matching the Exchange 5.5 mailboxes being migrated. For each SID that cannot be matched, the wizard creates a disabled user object.

As Figure 4.19 shows, the wizard requires that you specify the server and logon information for the other organization (there is no Browse option to find the correct server). In addition, you can only select one target store per migration process, so if you want to spread your users over multiple stores on an Exchange 2000 Server, you must run multiple migration wizards or move the mailboxes later. You might find this requirement to be somewhat of a hassle—as there is no option to save your previous settings in a working project file (this functionality is provided by many third-party migration tools—just another advantage of investing in such a utility), so you must re-enter and select the settings each time you perform a migration batch. It is possible, however, to put together a control file to run the migration from a command line, giving you a slight bit of automation once you get the files properly edited.

Figure 4.19: The wizard requires you to specify the information for the Exchange 5.5 organization.

In the next dialog box, which Figure 4.20 shows, you will select the target AD container, and set the account and password options.

 You will not see this option if you clear the *Create/modify mailbox accounts* check box earlier in the wizard. If you clear this check box, the mailbox contents are migrated to the accounts that you select.

I have selected a random password so that it is not tied to the account name (which would be a security hole during migrations), and I am forcing the user to change his or her password on next logon.

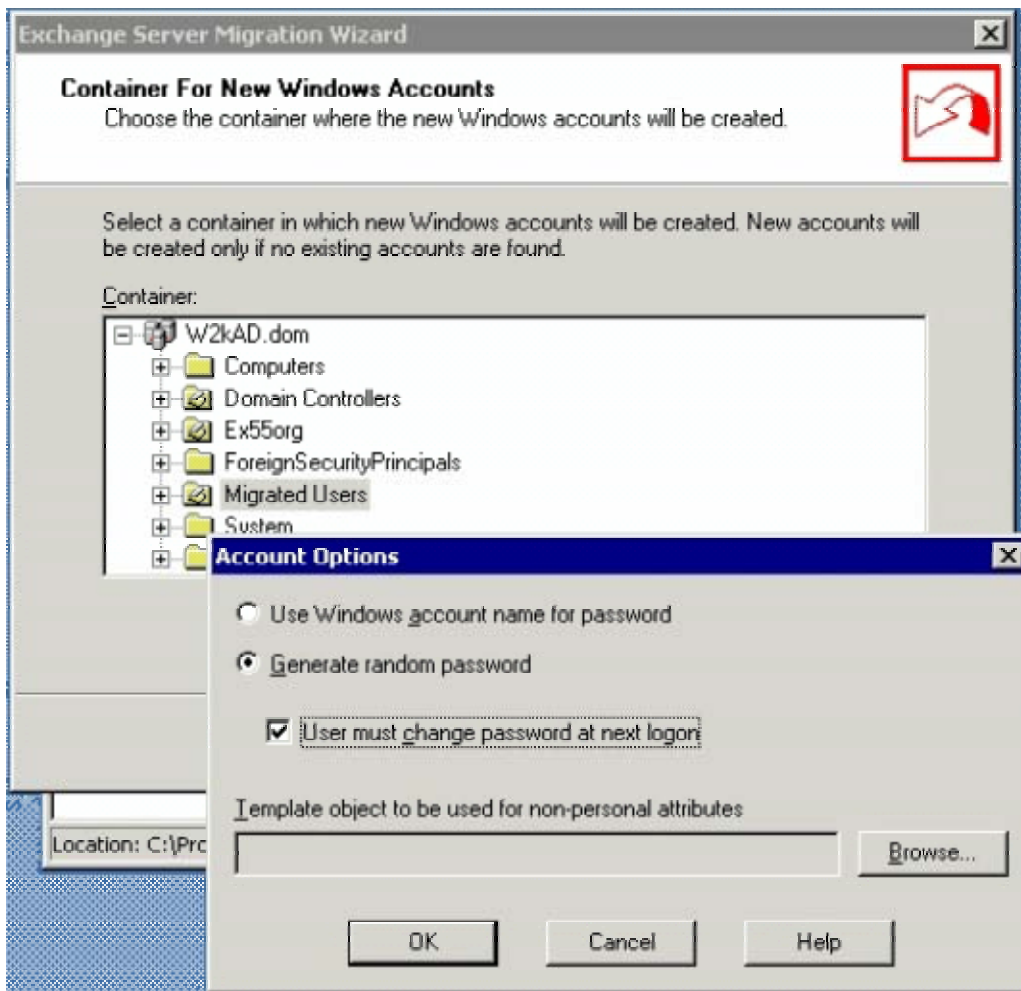


Figure 4.20: Setting container, account, and password options in the wizard.

Another important aspect of email migrations, and one that the wizard handles, is stamping the new account or mailbox with the old addresses (for example, SMTP, X.400, X.500) for the migrated mailbox. This feature is important for being able to reply to migrated email. These addresses must be secondary addresses so that the RUS does not overwrite them based on the default Recipient Policy. Also, keeping old addresses is an important consideration if you are investigating purchasing a third-party tool or are considering using a tool such as ExMerge for migration (because this tool does not automatically update account information).

Mailbox Migration Tips

This section provides a few tips or best practices for performing the mailbox migration. First, enable circular logging on the destination Exchange server or ensure that you have adequate free space on the transaction log drive. Be sure to perform a backup of the server both before you enable circular logging and after you turn it off (after you have migrated the mailboxes). For circular logging to take effect, you must stop and restart the Information Store service, which can be done from the command line:

```
NET STOP MSEXCHANGEIS & NET START MSEXCHANGEIS
```

The “&” strings the two commands together so that the start runs immediately after the service stops. This command will impact all Exchange users on that server—taking the server offline for a brief period.

In addition, you will not want ADC replication during the migration period, so either disable the replication in the CA or use the Services MMC snap-in to stop the ADC service.

Simply put, antivirus scanning will slow the migration process, as messages may be scanned on both the source and target destination. It is recommended that antivirus scanning be disabled during this process—however, if you disable antivirus software at the server or store level, your organization is left somewhat unprotected. Some antivirus scanning applications let you turn off antivirus scanning for individual mailbox selections. The latest antivirus scanning API (VSAPI2) in Exchange 2000 (covered in more detail in the next chapter) provides on-access scanning, meaning that the messages will be scanned when the email client attempts to open them. This feature ensures that no *known* viruses (with a signature in the antivirus scanner) will pass detection, making it safer to disable antivirus scanning during migration.

Prepare your users as much as possible about what to expect during the migration. You can develop preparation information for users during the pilot or testing phase of the migration. For example, you might want to provide preparation instructions about how to export rules (Inbox Assistant) from Outlook. Migrations require the re-creation of Outlook profiles; thus, offline folders (OSTs) will need to be completely rebuilt, preferably while the mobile user is connected to the high-speed network rather than a dial-up or VPN connection. Also educate the user community about what will happen if they have their Outlook profiles set to resolve addresses out of their personal address books or contacts instead of the GAL—as users are migrated, their addresses will change, so you must maintain the legacy address or it will break the personal address book or contact addressing.


Another tip is to use the message filtering capabilities of the Microsoft Exchange Migration Wizard or the third-party tool that you select to reduce the amount of old email that is migrated. Doing so is especially helpful if you have not been running any mailbox cleanup despite having a corporate policy on email retention.

Single Instance Storage

Single instance storage is the ability of Exchange server to store just one copy of a message (and more importantly, attachments) when the message is sent to multiple recipients. As long as the recipients do not modify and save the message, just one copy is saved. However, when you move users to a new server and new Exchange 2000 stores within that server, you will effectively eliminate the single instance storage. The multiple stores in Exchange 2000 each maintain a separate copy of each message, so single instance storage is impacted when you spread mailboxes across multiple stores.

So how do you assess the impact of the migration process on single instance storage? To start, you can estimate your current single instance storage ratio by using the counter available under MExchange Private Information Store in the NT or Windows performance monitor. However, this counter provides only the average number of pointers to each message and ignores one crucial detail—the size of each message. So messages of greater than, say, 1MB that have high single instance ratios have a greater benefit than messages of 1KB that have high single instance ratios. Thus, you can use this counter only to estimate your current ratio—not as an accurate measure of what will happen as you move users from Exchange 5.5 to Exchange 2000.

Finally, migration methods such as the move mailbox capability within Active Directory Users and Computers and the one-step method of the Microsoft Exchange Migration Wizard can actually maintain single instance storage for users moved within that session. However, if you run multiple sessions or if you move to multiple stores, single instance storage most likely will not be maintained. The same is true if you're using ExMerge to perform the migration—single instance storage will not be maintained because it effectively dumps the mail to a personal folder and then imports it. Most importantly, do not get too hung up on calculating the exact impact of single instance storage—simply allow some extra disk space overhead.

 Exmerge.exe is a very handy utility for moving and manipulating mailboxes. However, you should be aware of its limitations before you rely on it. Unlike the Microsoft Exchange Migration Wizard and third-party migration tools, for ExMerge to import the mailbox contents to the target server, the mailboxes must already exist. To initialize the new mailboxes, simply send an email to each new user (preferably via a distribution group).

Validation Procedures

To validate the success of the mailbox migration, the migration team lead should first check the size of the mailbox and the number of messages in the Exchange System Manager. In addition, migration teams can log on to a sample of mailboxes and check the following:

- Logon success—open mailbox
- Folders populated with existing mail, contacts, calendar items, and so on
- Items stored in profiles, such as rules, delegates, offline settings, and so on
- Ability to send new messages

- Ability to reply to existing messages, both externally and within the organization
- If you've performed an inter-organization migration and the Outlook profile must be re-created, the migration team might have to manually do so (if this task isn't handled by one of the profile automation tools)

Public Folders

When run in inter-org mode, the ADC does not synchronize Public Folders (or DLs), instead it creates contacts for them. This action allows users to email to Public Folders (or DLs) directly from the GAL, but it is up to you, the administrator, to set up Public Folder content synchronization. Note that permission settings are lost on the Public Folder content as you move them across forests. As the administrator, you should be careful of the sensitivity of the content—Microsoft has always been careful with limiting administrative control of Public Folder content and permissions between sites (for example, there are limitations within the DS/IS consistency adjuster to prevent a rogue administrator from taking over folders that do not belong in that site).

There is a tool in the SUPPORT\EXCHSYNC\I386 folder on the Exchange 2000 CD-ROM that is used for inter-organization Public Folder replication (such as Free/Busy). For more information, check out the Microsoft article “XGEN: Exchange 2000 Release Notes, Part II” (Q277845). Alternatively, you could take advantage of the ease with which many third-party tools handle this functionality.



This tool should not be confused with the InterOrg Synchronization tool (developed for Exchange 5.5) in the Microsoft BackOffice Resource Kit, Second Edition.

Another migration consideration is that if you start creating a hierarchy and content on the Exchange 2000 side, be sure to replicate the content to the Exchange 5.5 organization. The reason is to avoid a circumstance in which NT 4.0 users cannot access the content (in Exchange 2000) using their current NT 4.0 account authentication. As long as you have NT 4.0 accounts and Exchange 5.5 mailboxes, you will need to replicate Exchange 2000 Public Folders to the Exchange 5.5 organization.

Client Desktops and Outlook Profiles

Outlook profiles can be automatically updated when moving mailboxes to a new Exchange server within the same organization. The Outlook MAPI profile is automatically updated as long as the old server is still online to process the directory lookup. However, moves between organizations require you to reconfigure users' profiles. There are resource kit utilities such as profmod to perform this function (for example, via a logon script). In addition, third-party migration utilities offer this functionality.

Other Migration Considerations

During the migration, mail will be routed between the two organizations via SMTP. Thus, ensure that DNS records for each domain are configured with MX records. It is quite likely that you will already have your own Internet connector, but you might want to set up an SMTP connector within Exchange 2000 for the address space of the old organization, pointing directly to the Exchange 5.5 IMC.

As I have mentioned, in intra-organization migrations, DL migration consists of Universal Groups created in AD. In inter-organization migration, DLs are created as contacts with an external SMTP address (which means that you must not have already removed this address, something that we often did when performing security audits for Exchange organizations). You must maintain the membership on the originating Exchange 5.5 side (there is no two-way synchronization) until the list is moved to AD as a group.

Summary

In this chapter, we discussed the details of a migration scenario and covered some of the basic tools used during this process. In addition, we took a look at configuration and ongoing maintenance of accounts and mailboxes in multiple AD forests.

In the next chapter, we will look at best practices for taking care of AD and Exchange 2000 systems—from provisioning new systems and users to proactive maintenance and monitoring of the servers. We will cover the essential pieces of administration, including backups, disaster recovery, and antivirus and dealing with virus outbreaks.